UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA
FLORENCE DIVISION

Brooke Nielsen, Gerald Lee, and Chaya Clark, individually and on behalf of all others similarly situated, Plaintiffs, v. MEDNAX, Inc., MEDNAX Services, Inc., Pediatrix Medical Group, and American Anesthesiology, Inc. Defendants.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Brooke Nielsen ("Plaintiff Nielsen"), Gerald Lee ("Plaintiff Lee"), and Chaya Clark, as legal guardian of a minor child whose initials are C.J. ("Plaintiff Clark"), individually and on behalf of all other similarly situated individuals, and by and through their undersigned counsel file this Class Action Complaint against American Anesthesiology, Inc. ("AA"), Pediatrix Medical Group ("Pediatrix"), and MEDNAX Services, Inc. and MEDNAX, Inc. (collectively, "MEDNAX")[1], presumably the parent companies and/or business associates of Pediatrix and AA (collectively, "Defendants"), and allege the following based upon personal knowledge of facts and upon information and belief based upon the investigation of counsel as to all other matters.

NATURE OF THE ACTION

1. With this action, Plaintiffs seek to hold Defendants responsible for the harms they caused them and the nearly 1.3 million similarly situated persons in the massive and preventable

[1] MEDNAX, Inc. employees and MEDNAX Services, Inc. employees all use the same Microsoft Office 365 business email accounts that were the subject of this Data Breach (formatted as firstname_lastname@mednax.com) and, as such, the two MEDNAX entities are being collectively defined herein as "MEDNAX."

data breach that took place between June 17, 2020 and June 22, 2020 by which cyber criminals, through a phishing event, infiltrated Defendants' inadequately protected Microsoft Office 365-hosted business email accounts where sensitive personal information was being kept unprotected ("Data Breach" or "Breach").[2]

2. Defendants have also revealed that unauthorized third-parties accessed their business email accounts between October 20, 2019 to April 16, 2020, and October 13, 2015 to March 13, 2020,[3] and that Defendants experienced a separate data breach during the dates of July 2-3 of 2020.[4]

3. During the Data Breach period of June 17, 2020 through June 22, 2020, the cyber criminals gained access to certain of Defendants' Microsoft Office 365 business email accounts with the apparent intention of stealing protected personal information and protected health information of over a million individuals whose information was stored within one or more of these business email accounts.

4. MEDNAX is a physician-led healthcare organization that partners with hospitals, health systems and healthcare facilities to offer clinical services spanning the continuum of care, as well as revenue cycle management, patient engagement and perioperative improvement consulting solutions.[5] MEDNAX, Inc. is registered with the U.S. Security and Exchange Commission.

---

[2]The Data Breach appears on the U.S. Department of Health and Human Services' online public breach tool and shows that approximately 1,290,670 individuals were affected by the Data Breach. *See* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Feb. 1, 2021).

[3] https://emailevent.kroll.com/ (last accessed Feb. 4, 2021).

[4]https://www.oag.ca.gov/privacy/databreach/list?field_sb24_org_name_value=mednax&field_sb24_breach_date_value%5Bmin%5D%5Bdate%5D=&field_sb24_breach_date_value%5Bmax%5D%5Bdate%5D= (last accessed Jan. 22, 2021).

[5] https://www.mednax.com/about/ (last accessed January 8, 2021).

5. AA, formerly a MEDNAX company that was sold by MEDNAX to North American Partners in Anesthesia in May 2020,[6] is a "dynamic anesthesia partner that provides comprehensive, customized health solutions in a variety of clinical settings."[7] AA has more than 1,300 affiliated anesthesiologists and more than 2,000 affiliated advanced practice anesthesia providers in 15 states.[8] On its LinkedIn profile, AA still states that it is "part of MEDNAX."[9] However, the American Anesthesiology web page provided on the LinkedIn profile is currently inaccessible.

6. Pediatrix, a MEDNAX company, is the nation's largest provider of maternal-fetal, newborn and pediatric subspecialty services and delivers comprehensive, customized health solutions designed to enhance the patient experience. Pediatrix provides services to 41 states (including South Carolina) and Puerto Rico, employs over 1,975 physicians and over 1,050 advanced practice providers.

7. MEDNAX, Pediatrix, and AA collaborate (or, in the case of AA, collaborated in the past) with their partners and affiliates "to develop customized solutions that benefit hospitals, patients and payors." MEDNAX and Pediatrix tout on their website that they are "trusted by patients, hospitals, and referring physicians to *take great care of the patient, every day and in every way*."[10]

8. Plaintiffs and Class members were required, as patients of Defendants and their affiliate partners, to provide their "Personal and Medical Information" (defined below) to receive

---

[6] https://napaanesthesia.com/north-american-partners-in-anesthesia-napa-acquires-american-anesthesiology-from-mednax-inc-to-create-one-of-the-most-comprehensive-anesthesia-pain-management-and-perioperative-care-companies/ (last accessed Feb. 7, 2021).
[7] https://www.businesswire.com/news/home/20191018005359/en/American-Anesthesiology-a-MEDNAX-Company-to-Exhibit-at-the-ANESTHESIOLOGY%C2%AE-2019-Annual-Meeting-Oct.-19-21 (last accessed Feb. 7, 2021).
[8] *Id*.
[9] https://www.linkedin.com/company/american-anesthesiology (last accessed Feb. 4, 2021).
[10] *Id*.

medical and healthcare services, with the assurance that such information would be kept safe from unauthorized access. By taking possession and control of Plaintiffs' and Class members' Personal and Medical Information, Defendants assumed a duty to securely store and protect the Personal and Medical Information of Plaintiffs and the Class.

9. Defendants breached this duty and betrayed the trust of Plaintiffs and Class members by failing to properly safeguard and protect their Personal and Medical Information, thus enabling cyber criminals to access, acquire, appropriate, compromise, disclose, encumber, exfiltrate, release, steal, misuse, and/or view it.

10. The Personal and Medical Information at issue includes (i) patient contact information (such as patient name, guarantor name, address, email address, and date of birth); (ii) Social Security number, driver's license number, state identification number, and/or financial account information; (iii) health insurance information (payor name, payor contract dates, policy information including type and deductible amount and subscriber/Medicare/Medicaid number); (iv) medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Record Numbers); and (v) billing and claims information (invoices, submitted claims and appeals, and patient account identifiers used by the patient's provider).[11]

11. Defendants' misconduct – failing to timely implement adequate and reasonable data security measures to protect Plaintiffs' Personal and Medical Information, failing to timely detect the Data Breach, failing to take adequate steps to prevent and stop the Data Breach, failing to disclose the material facts that they did not have adequate security practices in place to safeguard the Personal and Medical Information, failing to honor their promises and representations to

[11] https://www.databreaches.net/?s=mednax (last accessed January 8, 2021).

protect Plaintiffs' and Class members' Personal and Medical Information, and failing to provide timely and adequate notice of the Data Breach – caused substantial harm and injuries to Plaintiffs and Class members across the United States.

12. Due to Defendants' negligence and failures, cyber criminals obtained and now possess everything they need to commit personal and medical identity theft and wreak havoc on the financial and personal lives of nearly 1.3 million individuals, many of which are babies and young children, for decades to come.

13. As a result of the Data Breach, Plaintiffs and Class members have already suffered damages. For example, now that their Personal and Medical Information has been released into the criminal cyber domains, Plaintiff Nielsen has experienced personal identity theft and Plaintiffs and Class members are at imminent and impending risk of both personal and medical identity theft. This risk will continue for the rest of their lives and, in Plaintiff Nielsen's case, has already begun to occur as described in further detail below.

14. Plaintiffs and Class members are now forced to deal with the ongoing danger of identity thieves possessing and using their Personal and Medical Information. Additionally, Plaintiffs and Class members have already lost time and money responding to and mitigating the impact of the Data Breach, which efforts are continuous and ongoing.

15. Plaintiffs bring this action individually and on behalf of the Class and seek actual damages, statutory damages, punitive damages, and restitution, with attorney fees, costs, and expenses, under certain state consumer protection and unfair and deceptive practices acts and data breach notification laws, and further sue Defendants for, among other causes of action, negligence and negligence *per se*. Plaintiffs also seek declaratory and injunctive relief, including significant improvements to Defendants' data security systems and protocols, future annual audits,

Defendant-funded long-term credit monitoring services, and other remedies as the Court sees necessary and proper. incurred in bringing this action, and all other remedies this Court deems proper.

THE PARTIES

16. Plaintiff Nielsen is a citizen and resident of the state of Virginia.

17. Plaintiff was a patient of AA in 2013 and 2016 for the births of her two children. At the time of her first child's birth, Plaintiff was very recently married, and it is likely that, due to the short turnaround of events, her maiden name was being used by AA on her medical records in AA's care. Importantly, the Notice of Data Breach letter sent to Plaintiff Nielsen was sent to her parents' address, not her current home address.

18. As required in order to obtain medical services from Defendants, Plaintiff Nielsen provided highly sensitive personal, health, and insurance information, including her Personal and Medical Information, to Defendants.

19. Plaintiff Nielsen received the Notice, dated January 13, 2021, from Defendants on or around January 21, 2021 informing her that her patient contact information, state identification number, health insurance information (payor name, payor contract dates, policy information, including type and deductible amount and subscriber/Medicare/Medicaid number), medical and/or treatment information (dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names, and Medical Record Numbers) and billing, payment, and claims information may have been compromised in the Data Breach. *See* **Exhibit 1**, the "Notice."

20. In October 2020, months after the Data Breach occurred but before Defendants had notified Plaintiff of the Data Breach, Plaintiff discovered that a total of twelve (12) Charles Schwab

bank accounts (six (6) high yield brokerage accounts and six (6) checking accounts) had been opened in her maiden name with her parents' address as the account owner's listed address.

21. Charles Schwab informed her that whoever had opened the accounts in her name had her name (with her maiden name), date of birth, Social Security number, parents' address, and parents' home phone number. Charles Schwab informed Plaintiff Nielsen that the day the accounts were opened was October 15, 2020.

22. Plaintiff immediately filed a police report with her local county police department and called three (3) credit bureaus to place freezes and fraud alerts on her accounts.

23. In January, Plaintiff received the Notice from AA and filed a second police report and was advised to submit her information to the Virginia Attorney General.

24. Plaintiff has since had a number of discussions with AA representatives regarding the Data Breach and it has become apparent from these discussions, and from the information that has been given to her by Charles Schwab regarding the bank accounts that were fraudulently opened in her name, that Plaintiff Nielsen's (and likely many other Data Breach victims') Social Security number was at risk of being compromised in the Data Breach.

25. Plaintiff Lee is a citizen and resident of the state of South Carolina.

26. Plaintiff Lee received the same or a similar Notice letter as the one Plaintiff Nielsen received in January 2021. See **Exhibit 2.**

27. Plaintiff Lee was a patient of AA in January 2017 for medical services he received at a community hospital in Knoxville, Tennessee.

28. As required in order to obtain medical services from Defendants, Plaintiff Lee provided highly sensitive personal, health, and insurance information, including his Personal and Medical Information, to Defendants.

29. Because of Defendants' negligence leading up to and including the period of the Data Breach, Plaintiff's Personal and Medical Information is now in the hands of cyber criminals and Plaintiff Lee is under an imminent and substantially likely risk of identity theft and fraud, including medical identity theft and medical fraud.

30. Plaintiff Clark and her minor child are citizens and residents of the state of South Carolina.

31. Plaintiff Clark received a letter dated December 16, 2020 from Defendants informing her that her minor children's name, address, date of birth, health insurance information (including payor name, payor contract dates, policy information including type and deductible amount and subscriber/Medicare/Medicaid number), medical and/or treatment information (including dates of service, location, services requested or procedures performed, diagnosis, prescription information, physician names and Medical Record Numbers), and billing and claims information were compromised in the Data Breach. See **Exhibit 3.**[12]

32. As required in order to obtain medical services from Defendants, Plaintiff Clark provided highly sensitive personal, health, and insurance information, including their children's Personal and Medical Information, to Defendants.

33. Because of Defendants' negligence leading up to and including the period of the Data Breach, Plaintiff's Personal and Medical Information is now in the hands of cyber criminals and J.C. is under an imminent and substantially likely risk of identity theft and fraud, including medical identity theft and medical fraud.

34. The imminent risk of medical identity theft and fraud that each Plaintiff and Class member now face is substantial, certainly impending, and continuous and ongoing because of the

[12] Plaintiff Clark has misplaced the notice she received. However Plaintiffs have attached a notice that is substantially similar to the one she received (including the same date).

negligence of Defendants, which negligence led to the Data Breach. Plaintiffs Nielsen, Lee, and Clark have already been forced to spend time responding to the Data Breach in an attempt to mitigate the harms of the Breach and determine how best to protect themselves from identity theft and medical information fraud. These efforts are continuous and ongoing.

35. As a direct and proximate result of the Data Breach, Defendants offered Plaintiffs Nielsen and Lee a woefully inadequate 12-month subscription to identity theft protection and credit monitoring. This subscription will need to be renewed yearly for the rest of Plaintiffs' lives in order to adequately protect them from the substantial, certainly impending, and continuous and ongoing risk of identity theft they now face. Plaintiff Clark has yet to be offered any identity theft protection and/or monitoring services.

36. Plaintiffs also suffered injury directly and proximately caused by the Data Breach, including damages and diminution in value of their Personal and Medical Information that was entrusted to Defendants for the sole purpose of obtaining medical services necessary for their health and well-being, with the understanding that Defendants would safeguard this information against disclosure. Additionally, Plaintiffs' Personal and Medical Information is at continued risk of compromise and unauthorized disclosure as it remains in the possession of Defendants and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect it.

37. Plaintiffs, to their knowledge, have never been victims of any type of identity theft before the occurrence of the Data Breach.

38. For the avoidance of doubt, any reference made in this Complaint to "Plaintiff Clark's Personal and Medical Information" or some variation thereof is to be interpreted as referring to the Personal and Medical Information of her minor child, J.C.

JURISDICTION AND VENUE

39. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d) because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and Plaintiffs and members of the Class are citizens of states that differ from Defendants.

40. This Court has personal jurisdiction over Defendants because Defendants conduct business in and have sufficient minimum contacts with South Carolina.

41. Venue is likewise proper as to Defendants in this District under 28 U.S.C. § 1391(a)(1) because a substantial part of the events or omissions giving rise to the claims asserted herein occurred in this District. Defendants conduct business through this District (including promoting, selling, marketing, and distributing the MEDNAX, AA, and Pediatrix brands and services at issue).

FACTUAL ALLEGATIONS

A. The Data Breach and Defendants' Failed Response

42. It is apparent from the Notice sent to Plaintiffs and the Class and from the sample "Notice of Data Security Incident" letters sent to state Attorneys General that the Personal and Medical Information stored within these Office 365 business email accounts was not encrypted.

43. Following the phishing event, Defendants began working with a forensic firm to investigate the Breach. Based upon the investigation, the hackers were able to access certain business email accounts between the dates of June 17, 2020 and June 22, 2020 where Plaintiffs' and Class members' Personal and Medical Information was being held, unencrypted and unprotected.

44. Defendants have also reported a subsequent data breach that took place from July 2, 2020 to July 3, 2020, along with a number of other data security intrusions that have taken place over the span of the last five years.

45. Upon information and belief, the unauthorized third-party gained access to the Personal and Medical Information and has engaged in (and will continue to engage in) misuse of the Personal and Medical Information, including marketing and selling Plaintiffs' and Class members' Personal and Medical Information on the dark web.

46. Despite knowing that over 1 million patients across the nation were in danger as a result of the Data Breach, Defendants did nothing to warn Plaintiffs or Class members until about half a year after learning of the Data Breach – an unreasonable amount of time under any objective standard.

47. Apparently, Defendants chose to complete their investigation and develop a list of talking points before giving Plaintiffs and Class members the information they needed to protect themselves against fraud and identity theft.

48. In spite of the severity of the Data Breach, Defendants have done very little to protect Plaintiffs and the Class, which is obvious by the subsequent data breach in July 2020 and the lack of any meaningful assistance offered to Plaintiffs and the Class. For example, in the Notice, Defendants only encourage victims "to carefully review credit reports and statements sent from providers as well as [victims'] insurance compan[ies] to ensure that all account activity is valid" and offer Plaintiffs Nielsen and Lee a woefully inadequate 12 months of identity theft monitoring.

49. In effect, Defendants are shirking their responsibility for the harm and increased risk of harm they have caused Plaintiffs and members of the Class, including the distress and financial burdens the Data Breach has placed upon the shoulders of the Data Breach victims.

50. Defendants failed to adequately safeguard Plaintiffs' and Class members' Personal and Medical Information, allowing cyber criminals to access this wealth of priceless information for nearly six months before warning the criminals' victims to be on the lookout, and now offer them little to no remedy or relief.

51. Defendants failed to spend sufficient resources on monitoring external incoming emails and training their employees to identify email-borne threats and defend against them.

52. Defendants had obligations created by HIPAA, reasonable industry standards, common law, state statutory law, and their assurances and representations to their patients to keep patients' Personal and Medical Information confidential and to protect such Personal and Medical Information from unauthorized access.

53. Plaintiffs and Class members were required to provide their Personal and Medical Information to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

54. The Personal and Medical Information at issue has great value to the hackers, due to the large number of individuals affected and the fact that health insurance information and Social Security numbers were part of the data that was compromised.

B. Defendants had an Obligation to Protect Personal and Medical Information under Federal and State Law and the Applicable Standard of Care

55. Defendants are covered by HIPAA (45 C.F.R. § 160.102). As such, they are required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part

164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

56. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

57. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

58. HIPAA requires Defendants to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

59. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

60. HIPAA's Security Rule requires Defendants to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by their workforce.

61. HIPAA also requires Defendants to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e).

62. HIPAA also requires Defendants to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

63. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendants to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[13]

64. Defendants were also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

65. As described before, Defendants are also required to protect Plaintiffs' and Class members' Personal and Medical Information, and further, to handle any breach of the same in accordance with applicable breach notification statutes.

66. In addition to their obligations under federal and state laws, Defendants owed a duty to Plaintiffs and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Personal and Medical Information in their possession

[13] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added).

from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Plaintiffs and Class members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems, networks, and protocols adequately protected the Personal and Medical Information of the Class.

67. Defendants owed a duty to Plaintiffs and the Class to design, maintain, and test their computer and business email systems to ensure that the Personal and Medical Information in Defendants' possession was adequately secured and protected.

68. Defendants owed a duty to Plaintiffs and the Class to create and implement reasonable data security practices and procedures to protect the Personal and Medical Information in their possession, including adequately training their employees and others who accessed Personal Information within their computer systems on how to adequately protect Personal and Medical Information.

69. Defendants owed a duty to Plaintiffs and the Class to implement processes that would detect a breach on their data security systems in a timely manner.

70. Defendants owed a duty to Plaintiffs and the Class to act upon data security warnings and alerts in a timely fashion.

71. Defendants owed a duty to Plaintiffs and the Class to adequately train and supervise their employees to identify and avoid any phishing emails that make it past their email filtering service.

72. Defendants owed a duty to Plaintiffs and the Class to disclose if their computer systems and data security practices were inadequate to safeguard individuals' Personal and Medical Information from theft because such an inadequacy would be a material fact in the decision to entrust Personal and Medical Information with Defendants.

73. Defendants owed a duty to Plaintiffs and the Class to disclose in a timely and accurate manner when data breaches occurred.

74. Defendants owed a duty of care to Plaintiffs and the Class because they were foreseeable and probable victims of any inadequate data security practices.

C. Defendants were on Notice of Cyber Attack Threats in the Healthcare Industry and of the Inadequacy of their Data Security

75. Defendants were on notice that companies in the healthcare industry were targets for cyberattacks.

76. Defendants were on notice that the FBI has recently been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[14]

77. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[15]

[14] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), http://www.reuters.com/article/2014/08/20/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820.

[15] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomeware-attacks-shut-down-clinics-hospitals.

78. As implied by the above quote from the AMA, stolen Personal and Medical Information can be used to interrupt important medical services themselves. This is an imminent and certainly impending risk for Plaintiffs and Class members.

79. Defendants were on notice that the federal government has been concerned about healthcare company data encryption. Defendants knew they kept protected health information in their email accounts and yet it appears Defendants did not encrypt these email accounts.

80. The United States Department of Health and Human Services' Office for Civil Rights urges the use of encryption of data containing sensitive personal information. As long ago as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, the DHHS's Office of Human Rights' deputy director of health information privacy, stated "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[16]

81. As covered entities or business associates under HIPAA, Defendants should have known about their weakness toward email-related threats and sought better protection for the Personal and Medical Information accumulating in their employees' business email accounts.

82. In the healthcare industry, the number one threat vector from a cyber security standpoint is phishing. Cybersecurity firm Proofpoint reports that "phishing is the initial point of compromise in most significant [healthcare] security incidents, according to a recent report from the Healthcare Information and Management Systems Society (HIMSS). And yet, 18% of

[16]"Stolen Laptops Lead to Important HIPAA Settlements," U.S. Dep't of Health and Human Services (Apr. 22, 2014), available at https://wayback.archive-it.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html.

healthcare organizations fail to conduct phishing tests, a finding HIMSS describes as 'incredible.'"[17]

83. The report from Proofpoint was published March 27, 2019, and summarized findings of recent healthcare industry cyber threat surveys and recounted good, common sense steps that the targeted healthcare companies should follow to prevent email-related cyberattacks.

84. One of the best protections against email related threats is security awareness training and testing on a regular basis. This should be a key part of a company's ongoing training of its employees. "[S]ince phishing is still a significant, initial point of compromise, additional work needs to be done to further lower the click rate," the HIMSS report states. "This can be done through more frequent security awareness training, phishing simulation, and better monitoring of metrics pertaining to phishing (including whether there are any particular repeat offenders)."[18]

85. ProtonMail Technologies publishes a guide for IT Security to small businesses (i.e., companies without the heightened standard of care applicable in the healthcare industry). In its 2019 guide, ProtonMail dedicates a full chapter of its e-book guide to the danger of phishing and ways to prevent a small business from falling prey to it. It reports:

> Phishing and fraud are becoming ever more extensive problems. A recent threat survey from the cybersecurity firm Proofpoint stated that between 2017 and 2018, email-based attacks on businesses increased 476 percent. The FBI reported that these types of attacks cost companies around the world $12 billion annually.
>
> Similar to your overall IT security, your email security relies on training your employees to implement security best practices and to recognize possible phishing attempts. This must be deeply ingrained into every staff member so that every time they check their emails, they are alert to the possibility of malicious action.[19]

---

[17] Aaron Jensen, *Healthcare Phishing Statistics: 2019 HIMSS Survey Results* (Mar. 27, 2019), https://www.proofpoint.com/us/security-awareness/post/healthcare-phishing-statistics-2019-himss-survey-results.
[18] *Id.*
[19] *The ProtonMail Guide to IT Security for Small Businesses*, PROTONMAIL (2019), available at https://protonmail.com/it-security-complete-guide-for-businesses.

86. The guidance that ProtonMail provides non-healthcare industry small businesses is likely still not adequate for companies like MEDNAX, Pediatrix, and AA, with the heightened healthcare standard of care based on HIPAA and the increased danger from the sensitivity and wealth of Personal and Medical Information they retain, but ProtonMail's guidance is informative for showing how inadequately Defendants protected the Personal and Medical Information of the Plaintiffs and the Class. ProofPoint lists numerous tools under the heading, "How to Prevent Phishing":

a. **Training:** "Training your employees on how to recognize phishing emails and what to do when they encounter one is the first and most important step in maintaining email security. *This training should be continuous as well. . . .*"

b. **Limit Public Information:** "Attackers cannot target your employees if they don't know their email addresses. Don't publish non-essential contact details on your website or any public directories . . . .

c. **Carefully check emails:** "First off, your employees should be skeptical anytime they receive an email from an unknown sender. Second, most phishing emails are riddled with typos, odd syntax, or stilted language. Finally, check the 'From' address to see if it is odd . . . . If an email looks suspicious, employees should report it."

d. **Beware of links and attachments:** "Do not click on links or download attachments without verifying the source first and establishing the legitimacy of the link or attachment…"

e. **Do not automatically download remote content:** "Remote content in emails, like photos, can run scripts on your computer that you are not expecting, and advanced hackers can hide malicious code in them. You should configure your email service provider to not automatically download remote content. This will allow you to verify an email is legitimate before you run any unknown scripts contained in it."

f. **Hover over hyperlinks:** "Never click on hyperlinked text without hovering your cursor over the link first to check the destination URL, which should appear in the lower corner of your window. Sometimes the hacker might disguise a malicious link as a short URL." [Proofpoint notes that there are tools online available for retrieving original URLs from shortened ones.]

g. **If in doubt, investigate:** "Often phishing emails will try to create a false sense of urgency by saying something requires your immediate action. However, if your employees are not sure if an email is genuine, they should not be afraid to take extra time to verify the email. This might include asking a colleague, your IT security lead, looking up the website of the service the

email is purportedly from, or, if they have a phone number, calling the institution, colleague, or client that sent the email."

h. **Take preventative measures:** "Using an end-to-end encrypted email service gives your business's emails an added layer of protection in the case of a data breach. A spam filter will remove the numerous random emails that you might receive, making it more difficult for a phishing attack to get through. Finally, other tools, like Domain-based Message Authentication, Reporting, and Conformance (DMARC) help you be sure that the email came from the person it claims to come from, making it easier to identify potential phishing attacks."[20]

87. As mentioned, these are basic, common-sense email security measures that every business, whether in healthcare or not, should be doing. By adequately taking these common-sense solutions, Defendants could have prevented this Data Breach from occurring.

D. Cyber Criminals Will Use Plaintiffs' and Class Members' Personal and Medical Information to Defraud Them

88. Plaintiffs and Class members' Personal and Medical Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiffs and the Class members and to profit off their misfortune.

[20] *Id.*

89. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[21] For example, with the Personal and Medical Information stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[22] These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and the Class members.

90. Personal and Medical Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.[23]

91. For example, it is believed that certain Personal and Medical Information compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma.[24]

92. The Personal and Medical Information exposed in this Data Breach are valuable to identity thieves for use in the kinds of criminal activity described herein.

93. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to personally identifiable information, they will use it.[25]

---

[21] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[22] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[23] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu

[24] *See https://www.engadget.com/stolen-data-used-for-unemployment-fraud-ring-174618050.html; see also* https://www.wired.com/story/nigerian-scammers-unemployment-system-scattered-canary/.

[25] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

94. However, hackers may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[26]

95. For instance, with a stolen Social Security number, which is part of the Personal and Medical Information compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[27] Identity thieves can also use the information stolen from Plaintiffs and Class members to qualify for expensive medical care and leave them and their contracted health insurers on the hook for massive medical bills.

96. Medical identity theft is one of the most common, most expensive, and most difficult to prevent forms of identity theft. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," which is more than identity thefts involving banking and finance, the government and the military, or education.[28]

97. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[29]

---

[26] *Data Breaches Are Frequent*, *supra* note 11.
[27] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.
[28] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/.
[29] *Id.*

98. As indicated by James Trainor, second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where [personal health information] can go from $20 say up to—we've seen $60 or $70 [(referring to prices on dark web marketplaces)]."[30] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market.[31]

99. If cyber criminals manage to steal financial information, health insurance information, and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendants have exposed the Plaintiffs and Class members.

100. A study by Experian found that the average total cost of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[32] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third saw their insurance premiums rise, and forty percent were never able to resolve their identity theft at all.[33]

---

[30] IDExperts, *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, https://www.idexpertscorp.com/knowedge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

[31] *Managing cyber risks in an interconnected world*, PRICEWATERHOUSECOOPERS: Key findings from The Global State of Information Security Survey 2015, https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

[32] *See* Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar, 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.

[33] *Id.*; *see also Healthcare Data Breach: What to Know About them and What to Do After One*, EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

101. As described above, identity theft victims such as Plaintiff Nielsen must spend countless hours and large amounts of money repairing the impact to their credit.[34]

102. The danger of identity theft is compounded when, like here, a minor's Personal and Medical Information is compromised, because minors typically have no credit reports to monitor. Thus, it can be difficult to monitor because a minor cannot simply place an alert on their credit report or "freeze" their credit report when no credit report exists.

103. With this Data Breach, identity thieves have already started to prey on the victims of the Data Breach, and one can reasonably anticipate this will continue.

104. Defendants' offer of one year of identity theft monitoring to only a limited number of Class members is woefully inadequate, as the worst is yet to come.

105. Victims of the Data Breach, like Plaintiffs and other Class members, must now spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their credit because of the Data Breach.[35]

106. In fact, as a direct and proximate result of the Data Breach, Plaintiffs and the Class have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs and the Class must now take the time and effort and spend the money to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services not offered to them by Defendants, or purchasing identity theft and credit monitoring services at the soon-to-be-expiration of the 12-month free monitoring period offered by Defendants, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, healthcare providers, closing or

[34] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.
[35] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

107. Plaintiffs and the Class will suffer, have suffered, and will continue to suffer, actual harms for which they are entitled to compensation, including:

a. Trespass, damage to, and theft of their personal property including Personal and Medical Information;

b. Improper disclosure of their Personal and Medical Information;

c. Injury resulting from actual identity theft;

d. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Personal and Medical Information being placed in the hands of criminals and having been already misused;

e. The imminent and certainly impending risk of having their confidential medical information used against them by spam callers to defraud them;

f. Damages flowing from Defendants untimely and inadequate notification of the data breach;

g. Loss of privacy suffered as a result of the Data Breach;

h. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

i. Ascertainable losses in the form of deprivation of the value of patients' personal information for which there is a well-established and quantifiable national and international market;

j. The loss of use of and access to their credit, accounts, and/or funds;

k. Damage to their credit due to fraudulent use of their Personal and Medical Information; and

l. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

108. Moreover, Plaintiffs and Class members have an interest in ensuring that their information, which remains in the possession of Defendants, is protected from further breaches by the implementation of industry standard and statutorily compliant security measures and safeguards. Defendants have shown themselves to be wholly incapable of protecting Plaintiffs' and Class members' Personal and Medical Information.

109. Plaintiffs and Class members are desperately trying to mitigate the damage that Defendants have caused them but, given the kind of Personal and Medical Information Defendants made accessible to hackers, they are certain to incur additional damages. Because identity thieves have their Personal and Medical Information, Plaintiffs and all Class members will need to have identity theft monitoring protection for the rest of their lives. Some, including babies and young children, may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with this change.[36]

110. None of this should have happened. The Data Breach was preventable.

[36] *Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov. 16, 2015), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.

E. Defendants Could Have Prevented the Data Breach but Failed to Adequately Protect Plaintiffs' and Class Members' Personal and Medical Information

111. Data breaches are preventable.[37] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[38] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[39]

112. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[40]

113. Defendants required Plaintiffs and Class members to surrender their Personal and Medical Information – including but not limited to their names, addresses, Social Security numbers, medical information, and health insurance information – and were entrusted with properly holding, safeguarding, and protecting against unlawful disclosure of such Personal and Medical Information.

114. Many failures laid the groundwork for the success ("success" from a cybercriminal's viewpoint) of the Data Breach, starting with Defendants' failure to incur the effort

[37]Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012)
[38]*Id.* at 17.
[39]*Id.* at 28.
[40]*Id.*

and costs necessary to implement adequate and reasonable cyber security procedures and protocols necessary to protect Plaintiffs' and Class members' Personal and Medical Information.

115. Defendants maintained the Personal and Medical Information in a reckless manner. In particular, the Personal and Medical Information was maintained, stored, and/or exchanged, unencrypted, in Microsoft Office 365 business email accounts that were kept in a condition vulnerable to cyberattacks.

116. Defendants knew, or reasonably should have known, of the importance of safeguarding Personal and Medical Information and of the foreseeable consequences that would occur if Plaintiffs' and Class members' Personal and Medical Information was stolen, including the significant costs that would be placed on Plaintiffs and Class members as a result of a breach.

117. The mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class members' Personal and Medical Information was a known risk to Defendants, and thus Defendants were on notice that failing to take necessary steps to secure Plaintiffs' and Class members' Personal and Medical Information from those risks left that information in a dangerous condition.

118. Defendants disregarded the rights of Plaintiffs and Class members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that their business email accounts were protected against unauthorized intrusions; (ii) failing to disclose that they did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiffs' and Class members' Personal and Medical Information; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiffs and Class members prompt and accurate notice of the Data Breach.

CLASS ACTION ALLEGATIONS

119. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

120. Plaintiffs bring all claims as class claims under Federal Rule of Civil Procedure 23. Plaintiffs asserts all claims on behalf of the Nationwide Class, defined as follows:

> **All persons residing in the United States whose personal and medical information was compromised as a result of the MEDNAX, Pediatrix, and AA Data Breach that occurred in June 2020.**

121. Alternatively, Plaintiffs propose the following alternative classes by state, as follows:

> **[Name of State] Subclass: All residents of [name of State] whose personal and medical information was compromised as a result of the MEDNAX, Pediatrix, and AA Data Breach that occurred in June 2020.**

122. Also, in the alternative, Plaintiffs request additional subclasses as necessary based on the types of Personal and Medical Information that were compromised.

123. Excluded from the Nationwide Class and Subclasses are Defendants, any entity in which Defendants have a controlling interest, and Defendants' officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

124. Plaintiffs reserve the right to amend the above definitions or to propose alternative or additional subclasses in subsequent pleadings and motions for class certification.

125. The proposed Nationwide Class or, alternatively, the separate Statewide Subclasses (collectively referred to herein as the "Class" unless otherwise specified) meet the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

126. **Numerosity:** The proposed Class is believed to be so numerous that joinder of all members is impracticable. The proposed Subclass is also believed to be so numerous that joinder of all members would be impractical.

127. **Typicality:** Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all members of the Class were injured through Defendants' uniform misconduct. The same event and conduct that gave rise to Plaintiffs' claims are identical to those that give rise to the claims of every other Class member because Plaintiffs and each member of the Class had their sensitive Personal and Medical Information compromised in the same way by the same conduct of Defendants.

128. **Adequacy:** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the Class and proposed Subclasses that they seek to represent; Plaintiffs have retained counsel competent and highly experienced in data breach class action litigation; and Plaintiffs and Plaintiffs' counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

129. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult, if not impossible, for members of the Class individually to effectively redress Defendants' wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties

and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

130. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendants engaged in the wrongful conduct alleged herein;

b. Whether Defendants failed to adequately safeguard Plaintiffs' and the Class's Personal and Medical Information;

c. Whether Defendants' email and computer systems and data security practices and response to the Data Breach that were used to protect Plaintiffs' and Class members' Personal and Medical Information violated the FTC Act, HIPAA, and/or state laws and/or Defendants' other duties discussed herein;

d. Whether Defendants owed a duty to Plaintiffs and the Class to adequately protect their Personal and Medical Information, and whether they breached this duty;

e. Whether Defendants knew or should have known that their computer and network security systems and business email accounts were vulnerable to a data breach;

f. Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the Data Breach;

g. Whether Defendants breached contractual duties to Plaintiffs and the Class to use reasonable care in protecting their Personal and Medical Information;

h. Whether Defendants failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and the Class;

i. Whether Defendants continue to breach duties to Plaintiffs and the Class;

j. Whether Plaintiffs and the Class suffered injury as a proximate result of Defendants' negligent actions or failures to act;

k. Whether Plaintiffs and the Class are entitled to recover damages, equitable relief, and other relief;

l. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiffs and members of the Class and the general public;

m. Whether Defendants' actions alleged herein constitute gross negligence; and

n. Whether Plaintiffs and Class members are entitled to punitive damages.

CAUSES OF ACTION

COUNT I – NEGLIGENCE

131. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

132. Defendants solicited, gathered, and stored the Personal and Medical Information of Plaintiffs and the Class as part of the operation of their business.

133. Upon accepting and storing the Personal and Medical Information of Plaintiffs and Class members, Defendants undertook and owed a duty to Plaintiffs and Class members to exercise reasonable care to secure and safeguard that information and to use secure methods to do so.

134. Defendants had full knowledge of the sensitivity of the Personal and Medical Information, the types of harm that Plaintiffs and Class members could and would suffer if the Personal and Medical Information was wrongfully disclosed, and the importance of adequate security.

135. Plaintiffs and Class members were the foreseeable victims of any inadequate safety and security practices. Plaintiffs and the Class members had no ability to protect their Personal and Medical Information that was in Defendants' possession. As such, a special relationship existed between Defendants and Plaintiffs and the Class.

136. Defendants were well aware of the fact that cyber criminals routinely target large corporations through cyberattacks in an attempt to steal sensitive personal and medical information.

137. Defendants owed Plaintiffs and the Class members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard such data and providing notification to Plaintiffs and the Class members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

138. Defendants' duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement

(Second) of Torts § 302B. Numerous courts and legislatures also have recognized the existence of a specific duty to reasonably safeguard personal information.

139. Defendants had duties to protect and safeguard the Personal and Medical Information of Plaintiffs and the Class from being vulnerable to cyberattacks by taking common-sense precautions when dealing with sensitive Personal and Medical Information. Additional duties that Defendants owed Plaintiffs and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendants' networks, systems, protocols, policies, procedures and practices to ensure that Plaintiffs' and Class members' Personal and Medical Information was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiffs' and Class members' Personal and Medical Information in their possession by using reasonable and adequate security procedures and systems;

c. To implement processes to quickly detect a data breach, security incident, or intrusion involving their business email system, networks and servers; and

d. To promptly notify Plaintiffs and Class members of any data breach, security incident, or intrusion that affected or may have affected their Personal and Medical Information.

140. Only Defendants were in a position to ensure that their systems and protocols were sufficient to protect the Personal and Medical Information that Plaintiffs and the Class had entrusted to them.

141. Defendants breached their duties of care by failing to adequately protect Plaintiffs' and Class members' Personal and Medical Information. Defendants breached their duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the Personal and Medical Information in their possession;

b. Failing to protect the Personal and Medical Information in their possession using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit, test, and train their employees to avoid phishing emails;

d. Failing to use adequate email security systems, including healthcare industry standard SPAM filters, DMARC enforcement, and/or Sender Policy Framework enforcement to protect against phishing emails;

e. Failing to adequately and properly audit, test, and train their employees regarding how to properly and securely transmit and store Personal and Medical Information;

f. Failing to adequately train their employees to not store Personal and Medical Information in their email inboxes longer than absolutely necessary for the specific purpose that it was sent or received;

g. Failing to consistently enforce security policies aimed at protecting Plaintiffs' and the Class's Personal and Medical Information;

h. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;

i. Failing to promptly notify Plaintiffs and Class members of the Data Breach that affected their Personal and Medical Information.

142. Defendants' willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

143. As a proximate and foreseeable result of Defendants' grossly negligent conduct, Plaintiffs and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

144. Through Defendants' acts and omissions described herein, including but not limited to Defendants' failure to protect the Personal and Medical Information of Plaintiffs and Class members from being stolen and misused, Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure the Personal and Medical Information of Plaintiffs and Class members while it was within Defendants' possession and control.

145. Further, through their failure to provide timely and clear notification of the Data Breach to Plaintiffs and Class members, Defendants prevented Plaintiffs and Class members from taking meaningful, proactive steps to securing their Personal and Medical Information and mitigating damages.

146. As a result of the Data Breach, Plaintiffs and Class members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, paying for credit monitoring and identity theft prevention services that, in most cases, were not offered to them by Defendants, and closely reviewing and monitoring bank accounts, credit reports, and statements sent from providers and their insurance companies.

147. Defendants' wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

148. Plaintiffs and the Class have suffered damages (as alleged above) in an amount to be determined at trial. These damages are the direct and proximate result of Defendants' grossly negligent conduct.

COUNT II – NEGLIGENCE PER SE

149. In addition to its duties under common law, Defendants had additional duties imposed by statute and regulations, including the duties under HIPAA and the FTC Act. The harms which occurred as a result of Defendants' failure to observe these duties, including the loss of privacy, significant risk of identity theft, and Plaintiffs' overpayment for goods and services, are the types of harm that these statutes and their regulations were intended to prevent.

150. Defendants violated these statutes when they engaged in the actions and omissions alleged herein and Plaintiffs' injuries were a direct and proximate result of Defendants' violations of these statutes.

151. Pursuant to the FTC Act, 15 U.S.C. § 45(a), Defendants owed a duty to Plaintiffs and the Class to provide fair and adequate computer systems and data security to safeguard the Personal and Medical Information of Plaintiffs and the Class.

152. Defendants are entities covered by HIPAA (45 C.F.R. §160.102) and, as such, are required to comply with HIPAA's Privacy Rule and Security Rule. HIPAA requires Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). HIPAA also requires Defendants to obtain satisfactory assurances that their business associates would appropriately safeguard the protected health information they receive or create on behalf of the Defendants. 45

C.F.R. §§ 164.502(e), 164.504(e), 164.532(d) and (e). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

153. HIPAA further requires Defendants to disclose the unauthorized access and theft of the protected health information of Plaintiffs and the Class "without unreasonable delay" so that Plaintiffs and Class members could take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their personal information. *See* 45 C.F.R. §§ 164.404, 164.406, and 164.410.

154. The FTC Act prohibits "unfair practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect Personal and Medical Information. The FTC publications and orders described above also formed part of the basis of Defendants' duty in this regard.

155. Defendants gathered and stored the Personal and Medical Information of Plaintiffs and the Class as part of their business of soliciting their services to their patients, which solicitations and services affect commerce.

156. Defendants violated the FTC Act by failing to use reasonable measures to protect the Personal and Medical Information of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

157. Defendants breached their duties to Plaintiffs and the Class under the FTC Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiffs' and Class members' Personal and Medical Information, and by failing to provide prompt notice without reasonable delay.

158. Defendants' failure to comply with applicable laws and regulations constitutes negligence *per se*.

159. Plaintiffs and the Class are within the class of persons that HIPAA and the FTC Act were intended to protect.

160. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act and HIPAA were intended to guard against.

161. Defendants breached their duties to Plaintiffs and the Class under these laws by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and the Class's Personal and Medical Information.

162. Additionally, Defendants had a duty to promptly notify victims of the Data Breach. For instance, HIPAA required Defendants to notify victims of the Breach within sixty (60) days of the discovery of the Data Breach. Defendants did not notify Plaintiffs or Class members of the Data Breach until around December 16, 2020.

163. Defendants knew on or before June 17, 2020, that unauthorized persons had accessed and/or viewed or were reasonably likely to have accessed and/or viewed private, protected, personal information of Plaintiffs and the Class.

164. Defendants breached their duties to Plaintiffs and the Class by unreasonably delaying and failing to provide notice expeditiously and/or as soon as practicable to Plaintiffs and the Class of the Data Breach.

165. Defendants' violation of the FTC Act and HIPAA constitutes negligence *per se*.

166. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, damages arising from the Data Breach, as alleged above.

167. The injury and harm that Plaintiffs and Class members suffered (as alleged above) was the direct and proximate result of Defendants' negligence *per se*.

168. Plaintiffs and the Class have suffered injury and are entitled to actual and punitive damages in amounts to be proven at trial.

COUNT III – UNJUST ENRICHMENT

169. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

170. Plaintiffs and the Class bring this claim in the alternative to all other claims and remedies at law.

171. Plaintiffs and Class members conferred a monetary benefit upon Defendants in the form of monetary payments to obtain medical services from Defendants.

172. Defendants collected, maintained, and stored the Personal and Medical Information of Plaintiffs and Class members and, as such, Defendants had direct knowledge of the monetary benefits conferred upon them by Plaintiffs and Class members.

173. Defendants, by way of their affirmative actions and omissions, including their knowing violations of their express or implied contracts with Plaintiffs and the Class members, knowingly and deliberately enriched themselves by saving the costs they reasonably and contractually should have expended on HIPAA compliance and reasonable data privacy and security measures to secure Plaintiffs' and Class members' Personal and Medical Information.

174. Instead of providing a reasonable level of security, training, and protocols that would have prevented the Data Breach, as described above and as is common industry practice among companies entrusted with similar Personal and Medical Information, Defendants, upon information and belief, instead consciously and opportunistically calculated to increase their own

profits at the expense of Plaintiffs and Class members (and continue to do so by electing to not provide free credit monitoring services to a majority of Class members negatively impacted by the Data Breach).

175. As a direct and proximate result of Defendants' decision to profit rather than provide adequate data security, Plaintiffs and Class members suffered and continue to suffer actual damages in (i) the amount of the savings and costs Defendants reasonably and contractually should have expended on data security measures to secure Plaintiffs' Personal and Medical Information, (ii) time and expenses mitigating harms, (iii) diminished value of Personal and Medical Information, (iv) loss of privacy, and (v) an increased risk of future identity theft.

176. Defendants, upon information and belief, have therefore engaged in opportunistic, unethical, and immoral conduct by profiting from conduct that they knew would create a significant and highly likely risk of substantial and certainly impending harm to Plaintiffs and the Class in direct violation of Plaintiffs' and Class members' legally protected interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendants to retain the benefits they derived as a consequence of their breach.

177. Accordingly, Plaintiffs and the Class are entitled to relief in the form of restitution and disgorgement of all ill-gotten gains, which should be put into a common fund to be distributed to Plaintiffs and the Class.

COUNT IV – BREACH OF CONTRACT

178. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

179. Plaintiffs and the Class entered into contracts with Defendants and provided payment to Defendants in exchange for Defendants' provision of medical services.

180. The promises and representations described above relating to compliance with HIPAA and industry practices, and about Defendants' concern for their patients' privacy rights, became terms of the contract between them and their patients, including Plaintiffs and the Class.

181. Defendants breached these promises by failing to comply with HIPAA and reasonable industry practices.

182. As a result of Defendants' breach of these terms, Plaintiffs and the Class have been seriously harmed and put at grave risk of debilitating future harms.

183. Plaintiffs and Class members are therefore entitled to damages in an amount to be determined at trial.

COUNT V – BREACH OF IMPLIED CONTRACT
(ALTERNATIVELY, TO COUNT IV)

184. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

185. When Plaintiffs and the Class members provided their Personal and Medical Information to Defendants when seeking medical services, they entered into implied contracts in which Defendants agreed to comply with their statutory and common law duties to protect Plaintiffs' and Class members' Personal and Medical Information and to timely notify them in the event of a data breach.

186. Defendants required their patients to provide Personal and Medical Information in order to receive medical services from their affiliate doctors and clinicians.

187. Defendants affirmatively represented that they collected and stored the Personal and Medical Information of Plaintiffs and the members of the Class in compliance with HIPAA and other statutory and common law duties, and using reasonable, industry standard means.

188. Based on the implicit understanding and also on Defendants' representations (as described above), Plaintiffs and the Class accepted Defendants' offers and provided Defendants with their Personal and Medical Information.

189. Plaintiffs and Class members would not have provided their Personal and Medical Information to Defendants had they known that Defendants would not safeguard their Personal and Medical Information, as promised, or provide timely notice of a data breach.

190. Plaintiffs and Class members fully performed their obligations under the implied contracts with Defendants.

191. Defendants breached the implied contracts by failing to safeguard Plaintiffs' and Class members' Personal and Medical Information and by failing to provide them with timely and accurate notice of the Data Breach.

192. The losses and damages Plaintiffs and Class members sustained (as described above) were the direct and proximate result of Defendants' breach of the implied contract with Plaintiffs and Class members.

COUNT VI – BREACH OF CONFIDENCE

193. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

194. At all times during Plaintiffs' and Class members' interactions with Defendants, Defendants were fully aware of the confidential nature of the Personal and Medical Information that Plaintiffs and Class members provided to Defendants.

195. As alleged herein and above, Defendants' relationship with Plaintiffs and the Class was governed by promises and expectations that Plaintiffs and Class members' Personal and Medical Information would be collected, stored, and protected in confidence, and would not be

accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

196. Plaintiffs and Class members provided their respective Personal and Medical Information to Defendants with the explicit and implicit understandings that Defendants would protect and not permit the Personal and Medical Information to be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

197. Plaintiffs and Class members also provided their Personal and Medical Information to Defendants with the explicit and implicit understandings that Defendants would take precautions to protect their Personal and Medical Information from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing, such as following basic principles of protecting their networks, data systems, and employee business email accounts.

198. Defendants voluntarily received, in confidence, Plaintiffs' and Class members' Personal and Medical Information with the understanding that the Personal and Medical Information would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by the public or any unauthorized third parties.

199. Due to Defendants' failure to prevent, detect, and avoid the Data Breach from occurring by, inter alia, not following best information security practices to secure Plaintiffs' and Class members' Personal and Medical Information, Plaintiffs' and Class members' Personal and Medical Information was accessed by, acquired by, appropriated by, disclosed to, encumbered by,

exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties beyond Plaintiffs' and Class members' confidence, and without their express permission.

200. As a direct and proximate cause of Defendants' actions and/or omissions, Plaintiffs and Class members have suffered damages as alleged herein.

201. But for Defendants' failure to maintain and protect Plaintiffs' and Class members' Personal and Medical Information in violation of the parties' understanding of confidence, their Personal and Medical Information would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties. Defendants' Data Breach was the direct and legal cause of the misuse of Plaintiffs' and Class members' Personal and Medical Information, as well as the resulting damages.

202. The injury and harm Plaintiffs and Class members suffered and will continue to suffer was the reasonably foreseeable result of Defendants' unauthorized misuse of Plaintiffs' and Class members' Personal and Medical Information. Defendants knew their data systems and protocols for accepting and securing Plaintiffs' and Class members' Personal and Medical Information had security and other vulnerabilities that placed Plaintiffs' and Class members' Personal and Medical Information in jeopardy.

203. As a direct and proximate result of Defendants' breaches of confidence, Plaintiffs and Class members have suffered and will suffer injury, as alleged herein, including but not limited to (a) actual identity theft; (b) the compromise, publication, and/or theft of their Personal and Medical Information; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Personal and Medical Information; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing

and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their Personal and Medical Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Class Members' Personal and Medical Information in their continued possession; (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (g) the diminished value of Defendants' services Plaintiffs and Class members received.

COUNT VII – BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING

204. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

205. As described above, Defendants made promises and representations to Plaintiffs and the Class that they would comply with HIPAA and other applicable laws and industry best practices.

206. These promises and representations became a part of the contract between Defendants and Plaintiffs and the Class.

207. While Defendants had discretion in the specifics of how they met the applicable laws and industry standards, this discretion was governed by an implied covenant of good faith and fair dealing.

208. Defendants breached this implied covenant when they engaged in acts and/or omissions that are declared unfair trade practices by the FTC and state statutes and regulations (including South Carolina's and Virginia's consumer protection acts), and when they engaged in

unlawful practices under HIPAA and other state personal and medical privacy laws. These acts and omissions included: representing that they would maintain adequate data privacy and security practices and procedures to safeguard the Personal and Medical Information from unauthorized disclosures, releases, data breaches, and theft; omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for the Class's Personal and Medical Information; and failing to disclose to the Class at the time they provided their Personal and Medical Information to them that Defendants' data security systems and protocols, including training, auditing, and testing of employees, failed to meet applicable legal and industry standards.

209. Plaintiffs and Class members did all or substantially all the significant things that the contract required them to do.

210. Likewise, all conditions required for Defendants' performance were met.

211. Defendants' acts and omissions unfairly interfered with Plaintiffs' and Class members' rights to receive the full benefit of their contracts.

212. Plaintiffs and Class members have been harmed by Defendants' breach of this implied covenant in the many ways described above, including overpayment for services, the purchase of identity theft monitoring services not provided by Defendants, imminent risk of certainly impending and devastating identity theft that exists now that cyber criminals have their Personal and Medical Information, and the attendant long-term time and expenses spent attempting to mitigate and insure against these risks.

213. Defendants are liable for this breach of these implied covenants, whether or not they are found to have breached any specific express contractual term.

214. Plaintiffs and Class members are entitled to damages, including compensatory damages and restitution, declaratory and injunctive relief, and attorney fees, costs, and expenses.

COUNT VIII – VIOLATIONS OF SOUTH CAROLINA UNFAIR TRADE PRACTICES ACT.

215. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

216. Plaintiffs bring this Count against Defendants on behalf of the South Carolina Subclass.

217. Defendants are "persons," as defined by S.C. Code Ann. § 39-5-10(a).

218. Defendants offer, sell, and distribute goods, services, and property, tangible or intangible, real, personal or mixed, and engage in trade and commerce that directly or indirectly affects the people of South Carolina. S.C. Code Ann. § 39-5-10(b).

219. Defendants, in the course of their business, engaged in unlawful practices in violation of S.C. Code Ann. § 39-5-20 (as guided by the interpretations given by the Federal Trade Commission and Federal Courts to Section 5(a)(1) of the FTC Act (15 U.S.C. 45(a)(1)), including unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.

220. Defendants' unlawful, unfair, and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class members' Personal and Medical Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous data incidents in the healthcare industry, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' Personal and Medical Information, including duties imposed by the FTC Act and HIPAA;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Class members' Personal and Medical Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' Personal and Medical Information, including duties imposed by the FTC Act and HIPAA;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Class members' Personal and Medical Information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' Personal and Medical Information, including duties imposed by the FTC Act and HIPAA.

221. Defendants' representations and omissions were material because they were likely to deceive reasonable patient consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of their Personal and Medical Information.

222. Defendants intended to mislead Plaintiffs and Class members and induce them to rely on their misrepresentations and omissions.

223. Had Defendants disclosed to Plaintiffs and Class members that their data security protocols and business emails (where highly sensitive personal data was exchanged and stored) were not secure and, thus, vulnerable to attack, Defendants would not have been able to continue in business and they would have been forced to adopt reasonable data security measures and comply with the law.

224. The above unlawful practices and acts by Defendants were immoral, unethical, oppressive, unscrupulous, and substantially injurious. These acts caused substantial and continuous injury to Plaintiffs and Class members.

225. Defendants acted intentionally, knowingly, and maliciously to violate South Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiffs' and the Class members' rights.

226. As a direct and proximate result of Defendants' unlawful practices, Plaintiffs and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including time and expenses related to monitoring their credit and medical accounts; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal and Medical Information.

227. Plaintiffs and South Carolina Subclass members therefore seek all monetary and non-monetary relief allowed by law under S.C. Code Ann. § 39-5-10 *et seq.* for Defendants violations alleged herein, including actual damages, civil penalties, and attorneys' fees and costs.

COUNT IX – VIOLATIONS OF S.C. CODE ANN. § 39-1-90.

228. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

229. Plaintiffs bring this Count against Defendants on behalf of the South Carolina Subclass.

230. Defendants are required to disclose to members of the South Carolina Subclass a data breach following discovery or notification of the breach in the security of the data, and such disclosure must be made "in the most expedient time possible and without unreasonable delay, consistent with … measures necessary to determine the scope of the breach and restore reasonable integrity to the data system." S.C. Code Ann § 39-1-90(A).

231. Defendants conduct businesses in South Carolina and own or license computerized data or other data that includes personal identifying information as set forth under S.C. Code Ann. § 39-1-90(A).

232. Plaintiffs' and South Carolina Subclass members' Personal and Medical Information (e.g., Social Security numbers) include personal information as covered under S.C. Code Ann. § 39-1-90(D)(3)(a).

233. Because Defendants were aware of the Data Breach (which caused or was reasonably likely to have caused the Personal and Medical Information to be acquired by an unauthorized person), Defendants had an obligation to disclose the Data Breach in a timely and expedient fashion or, at a minimum, in accordance with their own notification procedures, but failed in this obligation.

234. As a direct and proximate result of Defendants' violations of S.C. Code Ann. § 39-1-90, Plaintiffs and South Carolina Subclass members suffered damages, as described herein.

235. Plaintiffs seek relief under S.C. Code Ann. § 39-1-90(G), including actual damages, injunctive relief, and attorney fees, costs and expenses.

COUNT X – VIOLATIONS OF THE VIRGINIA CONSUMER PROTECTION ACT, VA. CODE ANN. § 59.1-196 *ET SEQ.*

236. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

237. Plaintiffs bring this Count against Defendants on behalf of the Virginia Subclass.

238. In the course of their business, Defendants engaged in deceptive acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement their offered health services, in violation of Va. Code Ann. § 59.1-196, including but not limited to the following:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class members' Personal and Medical Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous data incidents in the healthcare industry, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' Personal and Medical Information, including duties imposed by the FTC Act and HIPAA;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Class members' Personal and Medical Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members'

Personal and Medical Information, including duties imposed by the FTC Act and HIPAA;

f. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiffs' and Class members' Personal and Medical Information; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' Personal and Medical Information, including duties imposed by the FTC Act and HIPAA.

239. The above unlawful and deceptive acts were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

240. Defendants knew or should have known that their business email accounts, and data security practices were inadequate to safeguard Virginia Subclass members' Personal and Medical Information and that risk of a data breach or theft was highly likely.

241. Defendants' actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Virginia Subclass.

242. As a direct and proximate result of Defendants' deceptive practices, members of the Virginia Subclass suffered injury and damages.

243. Members of the Virginia Subclass seek relief under Va. Code Ann. § 59.1-204, including but not limited to, statutory damages, actual damages, and attorneys' fees and costs.

COUNT XI – DECLARATORY RELIEF

244. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

245. Plaintiffs bring this Count under the federal Declaratory Judgment Act, 28 U.S.C. §2201.

246. As previously alleged, Plaintiffs and members of the Class entered into an implied contract that required Defendants to provide adequate security for the Personal and Medical Information it collected from Plaintiffs and the Class.

247. Defendants owe a duty of care to Plaintiffs and the members of the Class that requires them to adequately secure Personal and Medical Information.

248. Defendants still possess Personal and Medical Information regarding Plaintiffs and members of the Class.

249. Since the Data Breach, Defendants have announced few if any changes to their data security infrastructure, processes or procedures to fix the vulnerabilities in their computer and email systems and/or security practices which permitted the Data Breach to occur and go undetected for months and, thereby, prevent further attacks.

250. Defendants have not satisfied their contractual obligations and legal duties to Plaintiffs and the Class. In fact, now that Defendants' insufficient data security is well-known to hackers, and considering Defendants' history of being susceptible to data security hacking incidents, the Personal and Medical Information in Defendants' possession remains highly vulnerable to cyberattack.

251. Actual harm has arisen in the wake of the Data Breach regarding Defendants' contractual obligations and duties of care to provide security measures to Plaintiffs and the

members of the Class. Further, Plaintiffs and the members of the Class are at risk of additional or further harm due to the exposure of their Personal and Medical Information and Defendants' failure to address the security failings that lead to such exposure.

252. There is no reason to believe that Defendants' security measures are any more adequate now than they were before the breach to meet Defendants' contractual obligations and legal duties.

253. Plaintiffs, therefore, seek a declaration that Defendants' existing security measures do not comply with their contractual obligations and duties of care to provide adequate security and that to comply with their contractual obligations and duties of care, Defendants must implement and maintain additional security measures.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class pray for judgment against Defendants as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Class requested herein;

b. A judgment in favor of Plaintiffs and the Class awarding them appropriate monetary relief, including actual and statutory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper.

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class and the general public as requested herein, including, but not limited to:

a. Ordering that Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendants audit, test, and train their security personnel regarding any new or modified procedures;

d. Ordering that Defendants segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendants' systems is compromised, hackers cannot gain access to other portions of Defendants' systems;

e. Ordering that Defendants cease transmitting Personal and Medical Information via unencrypted email;

f. Ordering that Defendants cease storing Personal and Medical Information in email accounts;

g. Ordering that Defendants purge, delete, and destroy in a reasonably secure manner customer data not necessary for their provisions of services;

h. Ordering that Defendants conduct regular database scanning and securing checks;

i. Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

j. Ordering Defendants to meaningfully educate their current, former, and prospective employees and subcontractors about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps they must take to protect themselves;

d. An order requiring Defendants to pay the costs involved in notifying the Class members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiffs and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all issues so triable.

DATED: February 17, 2021

[SIGNATURE TO FOLLOW]

THE LAW OFFICE OF KENNETH BERGER, LLC

s/ Elizabeth Dalzell
Kenneth E. Berger (Federal ID # 11083)
kberger@bergerlawsc.com
Elizabeth M. Dalzell (Federal ID # 7619)
edalzell@bergerlawsc.com
5205 Forest Drive, Suite 2
Columbia, SC 29206
803-790-2800

Counsel for Plaintiffs and the Proposed Class